UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/609,809	07/03/2000	Jeffrey Bruce Lotspiech	ARC9-2000-0063-US1	4266

7590 02/13/2004

John L Rogitz
Rogitz & Associates
750 B Street
Suite 3120
San Diego, CA 92101

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	2

DATE MAILED: 02/13/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/609,809	LOTSPIECH, JEFFREY BRUCE	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover she t with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 July 2000* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 July 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Pursuant to USC 131, claims 1-17 are presented for examination.

Oath/Declaration

1.1 Applicant has not given a post office address anywhere in the application papers as required by 37 CFR 1.33(a), which was in effect at the time of filing of the oath or declaration. A statement over applicant's signature providing a complete post office address is required.

Specification

2. The disclosure is objected to because of the following informalities: on page 8, second paragraph , and page 7, last paragraph, the following sentence needs to be corrected. "The result both changes ..."

On page 8, second paragraph, first sentence, diamond "28" should be replaced with diamond --32-- .

Appropriate correction is required.

Drawings

3. The drawings are objected to under 37 CFR 1.83(a) because they fail to show the second round of the cipher in the first iteration (when i=N) as described in the specification on page 8, second paragraph, last sentence. They also fail to show at the end of page 8 that odd numbers are used during forward and even rounds are used during backward chaining. Any structural

detail that is essential for a proper understanding of the disclosed invention should be shown in the drawing. MPEP § 608.02(d). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Objections

4. **Claims 8, 12, 14 and the intervening claims** are objected to because of the following informalities: on steps b(4) and e(4), act "(b)(1) should be corrected to avoid rendering the claim indefinite. Examiner will interpret it as (c)(1). Appropriate correction is required.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the

reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

5.1 **Claims 1-7, 11, and 13** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6,154,541 to **Zhang**.

5.2 **As per claim 1, Zhang** discloses a method that can be implemented for generating a tamper resistant version of a software program including a stream of data blocks, comprising: undertaking a predetermined number of iterations of forward plain text chaining of the blocks followed by backward plain text chaining of the blocks (see column 23, lines 30-57).

As per claim 2, Zhang discloses the limitation of further comprising XORing a first block with an adjacent block to render a chained block (see column 23, lines 30-57). With the use of DES the message is encrypted by XORing the ith byte of the message.

As per claim 3, Zhang discloses the limitation of further comprising scrambling chained blocks using a cipher (see column 23, lines 47-57).

As per claim 4, Zhang discloses the limitation of scrambling a chained block using at least one but not all rounds of the cipher to render a scrambled block before chaining the chained block to another block (see column 23, line 30 through column 24, line 5).

As per claim 5, Zhang discloses a permutation and scrambling operations during scrambling (see column 23, line 30 through column 24, line 5). **Zhang** also discloses descrambling (see column 23, lines 35-40). In descrambling the process is reversed to generate the initial plaintext. It is anticipated that to descramble the disclosure of **Zhang** meets the recitation of descrambling the chained block using only a single round of the cipher to render a result and then XORing the result with an adjacent block.

As per claim 6, Zhang discloses a cryptographic system (see drawing and column 6, lines 17-40) that meets the recitation of a computer program device, comprising: a computer program storage device including a program of instructions usable by an encryption computer, comprising: logic means for chaining a data block to a plain text version of an adjacent block in the stream to render a chained block (see column 23, lines 30-57); logic means for scrambling the chained block using a first round of a cipher to render a scrambled block (see column 23, line 30 through column 24, line 5); and logic means for iterating the means for scrambling and chaining using subsequent rounds of the cipher (see column 23, line 35 through column 24, line 5).

As per claim 7, Zhang discloses the limitation of wherein the means for iterating iterates forward and backward through the stream, using successive rounds of the cipher (see column 23, line 35 through column 24, line 5).

As per claim 11, Zhang discloses a method for generating a tamper resistant version of a software program including a stream of data blocks, comprising: providing a cipher defining rounds (see column 23, line 65 through column 24, line 5); iterating through the rounds of the cipher by iterating through respective outer loops of forward plain text chaining followed by backward plain text chaining (see column 23, line 31 through column 24, line 5); and during each forward portion of an outer loop, applying a respective round of the cipher to each block, and during each backward portion of an outer loop , applying a respective round of the cipher to each block (see column 23, line 65 through column 24, line 5).

As per claim 13, Zhang discloses a method for generating a tamper resistant version of a software program including a stream of data blocks, comprising: scrambling a block using one and only one round of a cipher (see column 23, line 30 through column 24, line 5); then chaining the block to another block to render a chained block (see column 23, lines 30-57); then scrambling the chained block using one and only round of the cipher (see column 23, line 30 through column 24, line 5).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have

been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6.1 **Claims 8-10, 12, 14, and 15-17** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,154,541 to **Zhang** in view of US Patent 6,333,983 to **Enichen et al.**.

6.2 **As per claims 8, 9, 12, 14, and 16, Zhang** substantially teaches a computer system for encrypting a stream of data blocks, comprising a processor programmed to execute method acts including: (a) receiving a sequence of N blocks (see column 23, lines 39-40); (b) initializing a previous block variable B (see column 23, line 48-50); (c) for i=1 to N, executing a DO loop comprising: (c)(1) XORing an ith block with B to render a modified ith block (see column 23, line 47-50); (c)(2) setting B equal to the modified ith block (see column 23, line 47-50); (c)(3) scrambling the modified ith block using at least one round of a cipher (see column 23, line 65 through column 24, line 5); (c)(4) incrementing "i" by unity and returning to act (c)(1) (see column 23, line 65 through column 24, line 5) **Zhang** discloses an example of BFSM it is anticipated that either backward or forward can be done first and forward implies $b_1 \ldots b_n$ which is incrementing "i"; (d) initializing a previous block variable B (see column 23, line 65 through column 24, line 5); (e) for i=N to 1, executing a DO loop comprising: (e)(1) XORing an ith block with B, yielding a modified ith block (e)(2) setting B to the modified ith block; (e)(3) scrambling the modified ith block using at least one next round of a cipher; (e)(4) decrementing "i" by unity

and returning to act (b)(1) (see column 23, line 65 through column 24, line 5); **Zhang** does not explicitly disclose in BFSM using XOR. However it is well known in the art and it is used in DES. In addition, **Zhang** discloses permutation and scrambling operations. **Enichen et al.** in an analogous art teaches XORing followed by scrambling (see figure 3). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the backward-forward chaining method of **Zhang** by replacing the permutation with XORing operation. The advantage is that it is easy to implement and economical. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Enichen et al.** so as to provide a backward-forward chaining method easy to implement and economical.

Zhang uses a loop to determine if the process reaches its end, but does not disclose returning to act (b) using a next round of the cipher. To repeat the process or add more rounds is apparent and well known in the art that one skill in the art would add another outside loop in order to predetermine a number of iterations to be executed. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Zhang** to determine whether a predetermined number of iterations have been executed, and if not, returning to act (b) using a next round of the cipher, otherwise outputting an encrypted stream of data blocks provide a backward-forward chaining method easy to implement and economical. This modification would have been obvious because one skilled in the art would have been motivated to provide more security but would not save in time and cost.

Claim 15 is a reverse process of the rejected claim 8 above wherein the decryption is used instead of encryption. **Zhang** discloses encryption with details and mentions without enough details how decryption can be accomplished by reversing the process of encryption. It is well known in the art that any encryption of a plaintext to a ciphertext can be decrypted with the reverse process to recover the plaintext. Therefore, claim 15 is rejected on the same rationale as the rejection of claims 8, 9, 10, 12, and 14 above. The step (b)(3) of determining if the next block exists does not have much or any weight since the input is a sequence of N blocks and the loop can determine the end of the block.

As per claims 10 and 17, Zhang discloses the limitation of wherein a respective round of the cipher is used for each iteration (see column 23, line 35, through column 24, line 5).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses the use of block ciphering with variable number of rounds.

US Patents:	6,185,679	Coppersmith et al.
	6,259,789	Paone

7.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 703-305-0355. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

cc

Carl Colin

Patent Examiner

February 6, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100